UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

UNITED STATES OF AMERICA	§	
	§	
v.	§	4:16-cr-00527
	§	
MARK DANIEL ADAIR	§	

ADAIR'S MOTION TO SUPPRESS, SUPPLEMENTAL BRIEFING

At the conclusion of yesterday's argument concerning Adair's motion to suppress (Doc. no. 61), the Court invited both parties to file a supplemental briefing. Adair files this supplement brief to show that (1) a search is either legal or illegal at its inception, (2) a search requiring a search warrant took place in this case, and (3) because the government exceeded the scope of 18 USC § 2703, the good faith exception should not apply.

I. THIS SEARCH WAS UNREASONABLE AT ITS INCEPTION.

"[I]n determining whether the seizure and search were 'unreasonable' our inquiry is a dual one—whether the officer's action was justified at its inception, and whether it was reasonably related in scope to the circumstances which justified the interference in the first place." *Terry v. Ohio*, 392 U.S. 1, 19–20 (1968); *see also New Jersey v. T.L.O.*, 469 U.S. 325, 341 (1985). Adair has argued that the search in this case was unjustified, based in part, on the fact that the subpoena issued for evidence by FBI Agent Mark Telle exceeded the bounds permitted by federal law.

As the subpoena itself notes, the subpoena was issued pursuant to 18 USC § 3486. That section of code permits the Attorney General to obtain certain files by

subpoena when investigating a "Federal offense involving the sexual exploitation or abuse of children. . ." *Id.* at (a)(i). Importantly, § 3486 (c) includes the following limitation:

> (C) A subpoena issued under subparagraph (A) with respect to a provider of electronic communication service or remote computing service, in an investigation of a Federal offense involving the sexual exploitation or abuse of children **shall not extend beyond**--
>
> > (i**) requiring that provider to disclose the information specified in section 2703(c)(2), which may be relevant to an authorized law enforcement inquiry**; or
> >
> > (ii) requiring a custodian of the records of that provider to give testimony concerning the production and authentication of such records or information.

Id.

> 18 USC § 2703 (c)(2) explains:
>
> (2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the--
>
> > (A) name;
> >
> > (B) address;
> >
> > (C) local and long distance telephone connection records, or records of session times and durations;
> >
> > (D) length of service (including start date) and types of service utilized;
> >
> > (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
> >
> > (F) means and source of payment for such service (including any credit card or bank account number),

> of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

Adair argues that a search carried out pursuant to this section of code, and without a warrant, is illegal and in violation of the Fourth Amendment. This argument is based on the precedent of *Riley v. California*, 134 S. Ct. 2473 (2014) and *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

However, there is a narrower ground upon which this motion could be granted: the search in this case was illegal because the government exceeded their authority under 18 USC §§ 2703 and 3486.

In addition to requesting the information permitted by federal law (which was requested on the face of the subpoena), the subpoena also ordered the production of the following information: "**any and all customer/subscriber/account holder information, all log in information, and any information that includes cloud computing. . . .**" *See* Doc. no 61, ex. 1, at 29 (emphasis added). This information was requested for three dates that spanning from December 16, 2015, until January 21, 2016. Nowhere does § 2703 permit any of these items to be obtained pursuant to a subpoena, and therefore the government's actions were in violation of the law that a subpoena "shall not extend beyond requiring that provider to disclose the information specified in section 2703(c)(2)." 18 USC § 3486.

The most troubling overreach is the demand for "any and all customer/subscriber/account holder information." This demand is broad enough include all information kept by the internet service provider for a citizen's account. It is well recognized that internet service providers store vast amounts of information about their customers, including their customer's browsing data. Dunlap, L., Cummings, J., & Janicki, T. N. (2018). Information Security and Privacy

Legislation: Current State and Future Direction. Journal of Information Systems Applied Research, 11(2), 24. This is why, "in 2016, legislation was passed that required ISPs to get permission from customers (or have them opt-in) whereas before the ISP could sell their data and browsing history." *Id.* at 25. This shows that even our federal representatives believed that information, such a browsing data, should be considered private.

In deciding whether or not a 4th Amendment search takes place, even when certain data is in the hands of a third party, the Supreme Court instructs us to consider "the nature of the particular documents sought to determine whether there is a legitimate 'expectation of privacy' concerning their contents." *Carpenter*, 138 S.Ct. at 2219 (internal quotations omitted). The Court noted that cell phones are now a "pervasive and insistent part of daily life" and that cell phone tracking data was being recorded without any action on the part of the cell phone user. *Id.* 2220. In much the same way internet browsing has been come both a pervasive and insistent part of daily life and service providers track online movements without any input from their customers.

In short, even if this Court believes that a subpoena strictly following the requirements 18 USC §§ 2703 and 3486 could pass constitutional muster, the subpoena in this case, by requesting any and all subscriber information, went too far and must be seen as a warrantless search which violates the Fourth Amendment.

II. THE GOOD FAITH DOCTRINE SHOULD NOT APPLY BECAUSE THE FBI DID NOT FOLLOW THE LAW.

The Supreme Court has made clear suppression is not proper for every Fourth Amendment violation. "Instead, the question turns on the culpability of the police and the potential of exclusion to deter wrongful police conduct." *Herring v. United States*, 555 U.S. 135, 137 (2009). One factor the Court instructs us to consider is the

deterrent effect of suppression. *Id.* at 141. The exclusionary rule should be applied to "curb police . . . misconduct" and when "the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional under the Fourth Amendment." *Id.* at 142-43 (quotations omitted). The question of whether to apply the exclusionary rule hinges on "the objectively ascertainable question whether a reasonably well-trained officer would have known that the search was illegal in light of 'all of the circumstances.'" *Id*.at 145 (citing Leon, 468 U.S., at 922, n. 23) (quotations omitted).

And the objectively reasonable well-trained officer would have known the subpoena used in Adair's case was illegally broad. The subpoena itself followed the law by requesting only the information permitted by 18 USC § 2703. However, by specifically adding Attachement A requesting information not authorized by § 2703 the issuing Special Agent exceeded his authority. Importantly, it is also clear that the reasonably well-trained officer would have known about the limitations of § 2703. The subpoena itself explains it is issued under the authority of 18 U.S.C. § 3486, (Doc no. 61, ex. 1 at 26), and § 3486 (c)(1) requires that a subpoena issued pursuant the statute "shall not extend beyond requiring that provider to disclose the information specified in section 2703(c)(2)." Simply reading the subpoena and the referenced law would have notified the reasonable officer that he could not demand any additional information, and certainly could not request "any and all customer/subscriber/account holder information."

Applying the exclusionary rule in this circumstance will create a deterrent effect by requiring that the FBI and other federal agents follow the letter of the law when relying upon administrative subpoenas.

Because the government failed to follow the mandates of 18 USC §§ 2703(c)(2) and 3486 they cannot rely upon the good faith exception to the exclusionary rule.

III. CONCLUSION

Mr. Adair requests that this Court find that he has standing to contest the search of his personal data in the possession of Comcast, and because that information was seized without a warrant, the seizure and search violated the Fourth Amendment and must be suppressed. Further, Mr. Adair request that this Court suppress the fruits of this illegal search, including all evidence obtained during the execution of the warrant on February 26, 2016, because the warrant was based upon the evidence illegally seized on December 16, 2015.

Respectfully submitted,

/s/ Neal Davis

Neal Davis
1545 Heights Blvd., Suite 700
Houston, Texas 77008
Office: (713) 227-4444
Cell: (713) 818-3780
Fax: (800) 760-7140
www.NealDavisLaw.com

Jonathan Landers
State Bar No. 24070101
Of Counsel with Neal Davis
917 Franklin St., Suite 300
Houston, Texas 77002
Email: jlanders.law@gmail.com

Defendant's lawyers

CERTIFICATE OF CONFERENCE

I certify I have emailed Assistant United States Attorney Kimberly Ann Leo about Adair's Motion to Continue and she is opposed.

/s/ NEAL DAVIS
Neal Davis

CERTIFICATE OF SERVICE

I certify that a copy of Adair's Motion to Suppress has been sent to all counsel of record on August 20, 2018 by email, and on August 20, 2018 via ECF/PACER.

/s/ Jonathan Landers
Jonathan Landers